IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT KNOXVILLE

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
	)	
v.	)	3:08-CR-142
	)	
	)	(PHILLIPS/SHIRLEY)
DAVID C. KERNELL,	)	
	)	
	)	
Defendant.	)	

REPORT AND RECOMMENDATION

All pretrial motions in this case have been referred to the undersigned pursuant to 28 U.S.C.§ 636(b) for disposition or report and recommendation regarding disposition by the District Court as may be appropriate. This case is before the Court on Defendant Kernell's Motion to Suppress Evidence for Which No Probable Cause Existed, Having Been Obtained Either Outside the Scope of Authority Granted by the Warrant or Under the Authority of an Unconstitutional General Exploratory Warrant ("First Motion to Suppress") [Doc. 20], filed on January 12, 2009,[1] and Second Motion to Suppress Evidence Obtained as Result of Government's Unauthorized Access of the Laptop Computer ("Second Motion to Suppress") [Doc. 69], filed on July 27, 2009. The Government responded [Doc. 22] in opposition to the first suppression motion on February 13, 2009. The Defendant filed a Reply [Doc. 27] on February 20, 2009. On July 16, 2009, the parties appeared

[1]The Court notes that the Defendant originally filed this motion on January 9, 2009 [Doc. 19] and then substituted the instant motion three days later.

before the undersigned for a hearing on the suppression motion. Assistant United States Attorneys D. Gregory Weddle, Mark Krotoski, and Josh Goldfoot appeared on behalf of the Government. Attorneys Wade V. Davies and Anne E. Passino represented the Defendant, who was also present. After hearing the arguments of the parties, the Court declined to hold an evidentiary hearing at that juncture and took the motion under advisement.

During the course of the July 16 hearing, the Defendant learned of the existence of a second search warrant for his laptop computer. On July 27, 2009, the defendant filed a Second Motion to Suppress Evidence Obtained as Result of Government's Unauthorized Access of the Laptop Computer [Doc. 69]. The Government responded [Doc. 72] in opposition to this motion on August 3, 2009, and the Defendant filed a reply [Doc. 74] on August 10, 2009. On August 23, 2009, the Defendant filed a supplement [Doc. 76] to his suppression motion pursuant to Local Rule 7.1(d).[2] The Government opposed [Doc. 78] the supplemental filing on August 25, 2009, arguing that it did not bring any new developments to the Court's attention.

On December 3, 2009, the Court heard the arguments of the parties on the second suppression motion. AUSA's Weddle, Krotoski, and Goldfoot were again present on behalf of the Government. Attorneys Davies and Passino again represented Defendant Kernell, who was also present. The Court also declined to hear any evidence at this time, finding it unnecessary to the Court's resolution of the motions. At the conclusion of the hearing, the Court took the motions

[2]Rule 7.1(d) prohibits supplemental filings without the Court's prior approval, with the exception of a brief of up to five pages "to call to the court's attention developments occurring after a party's final brief is filed." E.D.TN. LR 7.1(d). A response of up to five pages is due within five days. Id.

under advisement once more.

On January 7, 2010, the Defendant again supplemented [Doc. 101] his suppression motions, pursuant to Local Rule 7.1(d). The Government responded [Doc. 102] in opposition to the Defendant's second supplement the following day. Also on January 11, 2010, the Government filed its own supplement [Doc. 103] to its responses to the Defendant's suppression motions. After reviewing these supplemental filings, the Court again took the motions under advisement.[3]

I. BACKGROUND

This case arises out of Defendant David C. Kernell's alleged access of the Yahoo! email account of then Governor Sarah Palin[4] in September 2008. The following background information is taken primarily from the search warrants and related supporting documents, which were initially designated [Doc. 98] as sealed[5] exhibits in this case.

On September 20, 2009, Special FBI Agent Andrew M. Fischer sought a search warrant to

---

[3]On October 9, 2009, the Court declared [Doc. 86] this case to be complex for purposes of the Speedy Trial Act, due to the novel legal issues raised in the multiple pending dispositive motions, including the instant suppression motions. See 18 U.S.C. § 3161(h)(7)(B)(ii). In light of the complex legal questions that permeate this case and the additional motions that the Defendant has filed, the Court notes that the instant Report and Recommendation has not been and, indeed, could not be completed within the normal, thirty-day time frame contemplated in the typical case. See 18 U.S.C. § 3161(h)(1)(H), -(7)(B)(ii).

[4]Although Sarah Palin resigned her position as governor of Alaska during the pendency of this case, the Court will refer to her as Governor Palin in this report because that is how she is referenced in the Superseding Indictment and the parties' filings.

[5]At the Defendant's request, the Court previously designated [Doc. 98] these documents as sealed exhibits to the December 2, 2009 hearing. The Court unsealed the search warrants and attachments on March 31, 2010. The Court finds and the parties agree that references to the supporting affidavits are necessary for the Court to render this report. The supporting affidavits remain under seal, except for the Court's references contained herein, pending further order of the Court.

search the Defendant's bedroom and the common areas of the apartment in which the Defendant resided in Knoxville, Tennessee, in connection with his investigation of the Defendant's alleged unauthorized access of an email account belonging to Governor Palin. The undersigned United States Magistrate Judge found probable cause and issued the search warrant ("the first search warrant") that evening. Neither the search warrant and attachments, nor the supporting affidavit contained a search protocol limiting the way in which the computer would be analyzed. The search warrant was executed at 11:55 p.m., on September 20, 2008, and an Acer laptop computer was among the items seized from the Defendant's bedroom. Federal agents subsequently conducted a forensic analysis of the Defendant's computer.

On October 7, 2008, the Defendant was charged [Doc. 3] by indictment with a single count of felony unauthorized access of a computer. On February 3, 2009, the Defendant was charged in a four-count Superseding Indictment [Doc. 21], with identity theft, wire fraud, computer fraud, and anticipatory obstruction of justice. On February 26, 2009, Special FBI Agent Scott A. Wenger sought a search warrant to search the Defendant's laptop computer, previously seized as described above and remaining in the FBI's custody, for evidence of the new charges. The undersigned again found probable cause to issue the search warrant ("the second search warrant"), which issued that same day. The supporting affidavit stated that although targeted searches of computer data are possible in some cases, the affiant intended to use "whatever data analysis techniques appear necessary to locate an retrieve the evidence" named in the attachment.

II. POSITIONS OF THE PARTIES

The Defendant argues that the Fourth Amendment and Rule 41 of the Federal Rules of Criminal procedure require the suppression of the laptop computer seized from his apartment in September 2008 and all information gained through the offsite forensic searches of that computer. First, he challenges the execution of the first search warrant, contending that the executing officers exceeded the scope of the warrant by searching the entire contents of the computer. Procedurally, he argues that an evidentiary hearing is required to examine the extent and method of the search. He maintains that the second search warrant issued in February 2009 reveals that a particularized search was both required and feasible. Also, he contends that the Government disregarded the time limitations set out in both search warrants by searching beyond the ten days permitted by Rule 41 of the Federal Rules of Criminal Procedure. Second, and alternatively, he attacks the issuance of the first search warrant, asserting that if the search of his computer was within the scope of the first search warrant, then the issuing judge lacked probable cause to authorize a search of that breadth. In this regard, he argues that the first search warrant is a general warrant and that the government should have obtained a separate search warrant with a limiting search protocol immediately after the computer was seized.

The Government responds that the seizure and the search of the Defendant's laptop were both constitutional and properly within the scope of the first search warrant. It contends that an evidentiary hearing is unnecessary because the executing officers could and did search all of the files on the Defendant's computer for the evidence permitted by the search warrant. The Government argues that the Fourth Amendment does not require that a search warrant specify the precise manner of execution such as a search protocol. It contends that the second search warrant, which provided

additional judicial review and authorized a search for evidence of new statutory violations, simply provided additional protection to the Defendant. Although it acknowledges that the search of the Defendant's computer was not completed within ten days, it asserts that Rule 41's ten-day limitation on the execution of a search warrant does not apply to the further search of a hard drive that has already been seized. The Government maintains that if the Court finds that a constitutional violation has occurred, suppression of the evidence is not appropriate in this case because the executing agents acted in good faith. Finally, if suppression is warranted, then it should be limited to only that evidence seized pursuant to the overly broad portions of the search warrant.

III. ANALYSIS

The Fourth Amendment protects the right to be free from unreasonable searches and seizures. In this respect, a judge shall not issue a warrant for the search of a person, home, or personal property except upon a finding of "probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. Defendant Kernell contends that his rights under the Fourth Amendment were violated by the execution of both search warrants and by the issuance of the first search warrant. As to the execution of the search warrants, the Defendant argues that executing officers seized electronic materials beyond the scope of the first search warrant and conducted both searches in violation of time limitations contained in the two search warrants. With regard to the issuance of the first search warrant, the Defendant maintains that the judge lacked probable cause to issue a search warrant of that breath, which is devoid of a specific methodology for narrowing the search of the computer's contents.

A. Execution of the Search Warrants

The Defendant faults the search of his computer as being too broad and too long. As a predicate matter, the Defendant argues that to determine this issue, the Court must hold an evidentiary hearing to learn the extent and method of the forensic computer searches. Substantively, he argues that the first search warrant only authorized the seizure of his computer hardware and some of his computer files. Thus, he contends that the search executed in this case grossly exceeded the scope of the search warrant because agents searched entire contents of his computer and seized computer data not authorized by the search warrant. The Defendant also challenges the timing of the execution of both search warrants, contending that the forensic computer searches violated Rule 41 of the Federal Rules of Criminal Procedure because they extended beyond ten days.

(1) Necessity of Evidentiary Hearing.

The Defendant contends that an evidentiary hearing is necessary in this case to permit the Court to determine whether the execution of the first search warrant was reasonable. Specifically, in a section of his reply [Doc. 19] entitled Motion to Reveal Search Methodology, he asks the Court to require the Government "to disclose the identity of all government agents who have handled or examined Mr. Kernell's computer, the number of hours dedicated to these tasks, what they have found, and how they have gone about finding it." [Doc. 27, p.20] The Defendant argues that how the executing agents examined each file, "what keywords or other search methods and forensic programs were used, the time, extent, and whether any attempts were made to restrict the search results to the particularized files" are relevant to the question of whether the agents acted in disregard for the limitations of the original warrant. [Doc. 69, p.8] Finally, he contends that his

receipt in discovery of the forensic reports listing the computer data seized from his computer does not provide the necessary information on the extent of the search because the reports do not reveal the process that the agents undertook.

The Government responds that an evidentiary hearing is unnecessary in this case because no material issues of fact exist. It contends that executing agents searched all of the files on the Defendant's computer for the computer records particularly described in the warrant. It also agrees that the forensic examination of the Defendant's computer extended beyond ten days. The Government argues that the methods employed by those engaged in the forensic search(s) of the computer are not relevant to the issue of whether the agents had authority to search the entire computer. Accordingly, the Government asserts that the Defendant has failed to meet his burden of producing "'at least some initial showing of contested facts'" necessitating an evidentiary hearing. [Doc. 61, p.4 (quoting United States v. Giacalone, 853 F.2d 470, 482 (6th Cir. 1988)].

In August 2009, the Defendant raised for what appears to the Court to be the first time the issue that some items seized in the forensic analysis of his computer were not authorized by the search warrant, even if the agents were allowed to search through all of the computer's files. In his reply [Doc. 74] to the Government's response in opposition to the second suppression motion, the Defendant lists a number of items that he believes were not within the scope of the first search warrant. Moreover, he states that the forensic reports which disclose all the items seized from his computer suggest that the forensic examiner did not limit his search to just those items contained in Attachment B to the search warrant. He argues that these examples of problems with the execution of the first search warrant satisfy his burden to raise the issue of the agents exceeding the scope of the warrant.

At the December 3, 2009 hearing on the second suppression motion, the Defendant argued that an evidentiary hearing was necessary to determine whether the executing agents acted in flagrant disregard of the search warrant. He stated that he had now made a preliminary showing that items were seized that fall outside of the scope of the search warrant. The Defendant was permitted [Doc. 94] to place the forensic reports into the record as sealed exhibits to the hearing. The Government continued to argue that the steps the executing forensic analysts used to search the computer are not relevant. Instead, it argued that the relevant evidence is the end product–what the analysts seized from the computer, which evidence the Defendant had in the form of the forensic reports. The Government argued that in order to show the executing agents flagrantly disregarded the search warrant, the Defendant would have to show that the agents "seized" all the data on the Defendant's computer, which was not what occurred here.

The Court finds that an evidentiary hearing is not necessary to determine the essential issue in this case: Whether a search of all the files on the Defendant's computer exceeded the scope of the first search warrant. The Government acknowledges that the executing forensic computer analysts searched all of the files in the computer and did so for more than ten days after the issuance of each search warrant. The Court also finds that an evidentiary hearing is not necessary to determine whether probable cause existed to search the entire computer, an inquiry that turns upon the four corners of the supporting affidavit. United States v. Frazier, 423 F.3d 526, 531 (6th Cir. 2005) (whether a search warrant is supported by probable cause must be based solely upon an examination of the supporting affidavit). Finally, the Court finds that an evidentiary hearing is not necessary to determine whether certain items seized pursuant to the first search warrant exceeded its scope. The Court has before it both Attachment B, which states what the agents were allowed

to seize, the forensic reports that detail what was seized, and the Defendant's reply setting forth the items he contends were seized outside of the scope of the first search warrant.[6] Because the resolution of these issues involves no contested issue of fact, the Court concludes that an evidentiary hearing is not necessary. See United States v. Abboud, 438 F.3d 554, 557 (6th Cir. 2006).[7]

(2) Scope of Search

The Defendant contends that seizing and searching the entire contents of his laptop computer was unreasonable. In this regard, he asserts that (1) the agents should not have searched his computer offsite, (2) the agents should have employed a limiting search protocol rather than searching through all the files on the computer, (3) the agents seized computer data beyond that authorized by the search warrant, and (4) the agents did not act in good faith. The Court will examine each of these contentions in turn.

(i) Propriety of offsite search.

The Defendant first argues that the executing agents could have conducted a narrow search

[6]The Court notes that the Defendant characterizes these items as being those "limited examples" that he "can discern from what the government has chosen to include in its reports," thereby indicating that this list is not exclusive. Nevertheless, the Defendant is not entitled to an unlimited number of hearings or filings in which he might continue to discern additional items that he will claim exceed the scope. The Defendant has had Attachment B to the first search warrant, which lists the items that the agents were allowed to seize, since very early in this case. He has had the list of items that were seized in the forensic analysis of the computer since late June 2009. Thus, the Court will consider only those items listed in the Defendant's reply.

[7]Because the Court declined to hold an evidentiary hearing on July 16, 2009, or at any time on the suppression motions, the United State's Motion to Quash Subpoena to FBI Special Agents [Doc. 64] is moot.

onsite or made a mirror image of the computer, implying that the computer itself was improperly seized. Relying upon United States v. Guest, the Government responds that executing agents may constitutionally seize the entire computer (or a copy of it) for a later search offsite, even though such a seizure necessarily includes computer data not within the scope of the search warrant. 255 F.3d 325, 334-35 (6th Cir. 2001). The Court agrees with the Government that the Defendant's computer itself was properly seized as an alleged instrumentality of the crime.

Rule 41(c) of the Federal Rules of Criminal Procedure provides that a "warrant may be issued for"

> (1) evidence of a crime;
>
> (2) contraband, fruits of crime, or other items illegally possessed;
>
> (3) property designed for use, intended for use, or *used in committing a crime*; or
>
> (4) a person to be arrested or a person who is unlawfully restrained.

(Emphasis added). In the present case, the Agent Fisher's affidavit in support of the first search warrant expressly states that one of the Defendant's roommates reported the Defendant kept an Acer laptop computer in his room and that on September 17, 2008, the Defendant admitted to the roommate that he had broken into Governor Palin's email account. Another roommate stated that on September 16, the Defendant knocked on his bedroom door, asked him to come and look at a Yahoo! password retrieval site, and said he was about to get access to Governor Palin's email. The affidavit states that based upon the information stated therein, the Defendant's Acer laptop computer was used in the commission of the unauthorized access of Governor Palin's Yahoo! account and is, thus, an instrumentality of the crime. After reviewing the affidavit, the Court also concludes that the computer was properly seized as an instrumentality of the crime. See Fed. R. Crim. P. 41(c)(3).

The Sixth Circuit has upheld the seizure of a computer and the subsequent search of the computer off-site due to the "technical difficulties of conducting a computer search in a suspect's home[.]" Guest v. Leis, 255 F.3d 325, 334-35 (6th Cir. 2001). In so holding, the appellate court observed that such a procedure necessarily involved the seizure of computer data unrelated to the offenses. Id. at 334. The Government contends that every other circuit to consider the issue has also held that the seizure of a computer (or a copy of its hard drive) and its subsequent search offsite does not violate the Fourth Amendment. See United States v. Giberson, 527 F.3d 882, 886-87 (9th Cir. 2008) (holding that "where there was ample evidence that the documents authorized in the warrant could be found on [the defendant's] computer, the officers did not exceed the scope of the warrant when they seized the computer"); United States v. Grimmett, 439 F.3d 1263, 1269 (10th Cir. 2000) (holding that search warrant authorized both the seizure and offsite search of the computer); United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) (concluding that "[a]s a practical matter, the seizure and subsequent off-premises search of the computer and all available disks was about the narrowest definable search and seizure reasonably likely to obtain" the contraband sought, child pornography).

Defendant attempts to distinguish Guest, arguing that the present case is devoid of allegations that he was engaged in other criminal activity (such as pervasive fraud) that warranted a blanket authorization to search all of his files. He also points out that the information possessed by Agent Fischer revealed that the Defendant did not have sophisticated computer skills. The Court finds that these differences do not separate this case from Guest. While the Court will address whether the agents could properly search through all of the computer files for the items listed in the

warrant in the next subsection of the analysis, it here notes that Guest likewise did not involve criminal activity believed to permeate virtually all of the files on the seized computer. Id. at 330 (search for obscenity on computers containing an electronic bulletin board system, which permitted subscribers to send email, "participate in chat room conversations, on-line games, and conferences, where they could post or read messages on many topics, and they could download files such as computer programs and pictures"). Also, the analysis permitting the seizure and offsite search of the computer did not turn upon the sophisticated computer skills of the owner. Instead, the appellate court's decision turned upon the inability of the executing officers to readily separate the relevant computer files from the unrelated files while conducting the search in the defendant's home. Id. at 335. Indeed, the instant affidavit recognizes this fact:

> Computer storage devices (such as hard disks, diskettes, CD-ROMs , etc.) can store the equivalent of thousands of pages of information. Additionally, a user may seek to conceal criminal evidence by storing it in random order with deceptive file names. Searching authorities are required to examine all the stored data to determine which particular files are evidence, contraband, fruits, or instrumentalities of criminal activity. This sorting process can take weeks or months, depending on the volume of data stored; and it would be impractical to attempt this kind of data analysis on site.

Accordingly, the Court finds that the executing agents properly seized the Defendant's computer pursuant to the first search warrant as an instrumentality of the crime and properly searched it offsite.

(ii) Searching computer's entire contents vs employing a limiting protocol

The Defendant next argues that the agents grossly exceeded the scope of the first search warrant and, thus, transformed the warrant into a general exploratory warrant, requiring that all the

evidence seized from the search of his computer must be suppressed. He contends that the search warrant "did not authorize the wholesale examination of all files on his computer." [Doc. 20, p.6-7] Instead, he contends that the search warrant only permitted the executing agents to examine those files that contained the items listed in Attachment B. He maintains that the officers should have either employed a limiting methodology to insure that they were not searching irrelevant files or obtained a second, more particular search warrant once they seized the computer.

Attachment B to the first search warrant permitted, in pertinent part, the agents to search for the following:

> Documents and computer files any in [sic.] form including but not limited to e-mail, documentation or papers, and digital data that may related [sic.] or be associated the screen nicknames rubico and rubico10, the e-mail accounts rubico@yahoo.com and rubico10@yahoo.com, dkrocket@mindspring.com, gov.palin@yahoo.com; Governor Sarah Palin; Facebook; other internet accounts or online services or groups, or hacking activities.

The Defendant argues that all computer data not containing the above listed items was seized outside of the scope of the search warrant.

The Government responds that the search of the Defendant's computer did not exceed the scope of the search warrant. It contends that in authorizing the agents to search *for* particular computer records, the warrant authorized the agents to search *through* all of the Defendant's computer files for that information. It maintains that the agents could reasonably search through items not specified in the warrant in order to locate those items that were.

Initially, the Court observes that the affidavit supporting the first search warrant contains a three and one-half page section entitled "Specifics of Search and Seizure of Computer Systems. In this section, the affiant states that a search of a computer often requires the seizure of the computer

(or a copy of the hard drive) and subsequent "process[ing]" by an expert in a controlled environment. The affidavit states that this procedure is necessary "to completely and accurately retrieve data" because computers contain vast amounts of information and the user can conceal information by storing it randomly and using misleading file names. Additionally, experts and a controlled environment are required to search the computer in a way that both protects the integrity of the files and uncovers hidden or deleted materials.

Search warrants are typically concerned with what items may be seized, i.e., what the officers are searching for, rather than the method in which the officers execute the search: "The warrant process is primarily concerned with identifying *what* may be searched or seized– not how–and whether there is sufficient cause for the invasion of privacy thus entailed." Upham, 168 F.3d at 537. "A lawful search of fixed premises generally extends to the entire area in which the object of the search may be found and is not limited by the possibility that separate acts of entry or opening may be required to complete the search." United States v. Ross, 456 U.S. 798, 820-21 (1982).

When executing a search warrant, officers are permitted to look in any container or location on the premises that could hold the items to be seized, even if those containers are not specified in the search warrant. See United States v. McLavain, 310 F.3d 434, 439 (6th Cir. 2002) (finding search under a bed and in a garage to be objectively reasonable pursuant to a search warrant for a fugitive because a person could hide in these locations). In order to search a container, it must be reasonable that the item(s) listed in the search warrant could be found therein. Id.; Gilberson, 527 F.3d at 887-88. As the Supreme Court has noted with regard to searches for documents, the executing agent may examine some "innocuous" items "at least cursorily, in order to determine

whether they are, in fact, among those [items] authorized to be seized." Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976).

The Defendant argues that even if probable cause existed to search parts of his computer, the executing agents lacked probable cause to search other parts. Thus, he concludes that a search of the entirety of the data on his computer constituted an unjustified intrusion into his privacy, even if that search was conducted with an electronic device such as a forensic program. The Court disagrees. The supporting affidavit provided probable cause to believe that the items listed in Attachment B, which included certain computer data, would be located on the Defendant's computer. The affidavit provided a nexus between the Defendant's computer and the desired data listed in Attachment B by providing probable cause that the Defendant committed the unauthorized access of Governor Palin's account on his laptop computer. Thus, the search warrant properly authorized the executing agents to search through all of the compartments, i.e., the files or information packets as the Defendant calls them, in the computer for the items to be seized. Whether the agents used a forensic program to conduct the search or looked at each file to determine if it contained the information for which they were searching is inapposite because they had probable cause to look in the Defendant's computer.[8]

[8]The Defendant argues [Doc. 27, p.8] that the Government may not employ an electronic device (i.e., forensic search software) to gain information from an area in which a person enjoys a reasonable expectation of privacy (i.e., his computer) that could not be gained through sensory observation. See United States v. Karo, 468 U.S. 705, 717-18 (1984) (rejecting "Government's contention that it should be completely free from the constraints of the Fourth Amendment to determine by means of an electronic device, without a warrant and without probable cause or reasonable suspicion, whether a particular article-or a person, for that matter-is in an individual's home at a particular time"). The Court's reasoning is consistent with the case law referenced because the Court finds that the executing forensic analysts had probable cause to employ their forensic software to search all of the files on the Defendant's computer.

Thus, the Court concludes that when the search warrant permits the agents to search a computer, they may search all of the files in that computer for the items to be seized:

> Searching agents have the authority to look in any place where the evidence sought may be found. The methods employed in executing search warrants are left to the searching agent's discretion as long as the methods are reasonable. Contrary to Defendant's argument, [the executing officer] seized all of the computer equipment, not each individual file. This was proper because all of the computer equipment and storage devices were within the scope of the search warrant. [The executing officer] thus acted reasonably in executing the search warrant, and his examination of each file on Defendant's computers and storage media was reasonable and necessary.

United States v. Ogden, No. 06-20033-STA, 2008 WL 4982756, *3 (W.D. Tenn. Nov. 18, 2008) (holding that executing officer did not exceed the scope of the search warrant); see also Gilberson, 527 F.3d at 889-90 (holding that officers could search all the files on the computer for child pornography). "[S]o long as the computer search is limited to a search for evidence explicitly authorized in the warrant, it is reasonable for the executing officers to open the various types of files located in the computer's hard drive in order to determine whether they contain such evidence." United States v. Jack, No. S-07-0266, 2009 WL 453051, *4 (E.D. Cal. Feb. 29, 2009) (collecting cases).

The Government likens this case to United States v. Tillotson, No. 2:08-CR-33, 2008 WL 5140773 (E.D. Tenn. Dec. 2, 2008), in which agents seized the defendant's computer pursuant to a search warrant and then examined its entire contents off-site for evidence of child pornography. In Tillotson, the court found that due to the user's ability to assign misleading file names to the evidence sought, it was "necessary to search basically every file on the computer" to locate specific data such as child pornography. Id. at *4. The Court finds that the same is true in the present case: The executing agents necessarily had to search through all the files on the Defendant's computer to

locate the evidence of unauthorized access of Governor Palin's email account. Moreover, the supporting affidavit relates that an individual identifying himself as "rubico" and believed to be the Defendant stated on an internet chat site that he "was behind a proxy," with the implication being that he was disguising his identity. The affidavit also states that the individual claimed that he deleted the information taken from Governor Palin's account from his computer. These assertions indicate that the information sought on the Defendant's computer would not be located easily.

The Defendant seeks to distinguish Tillotson, by pointing to the differences in the "duration" of the evidence in the two cases. Consistent with Sixth Circuit precedent, Tillotson holds that the specificity required in the search warrant depends "upon in the types of items to be seized and the type of crime under investigation." Id. at *4; see also United States v. Henson, 848 F.2d 1374, 1383 (6th Cir. 1988). The Defendant argues that the Tillotson search warrant was properly less specific due to the nature of the items to be seized from Tillotson's computer (images of child pornography) and the fact that the crime in Tillotson was ongoing as opposed to an "isolated circumstance of brief duration." In contrast, he contends that this case involves a crime occurring during a very brief window of time on September 16, 2008.

Although the Court agrees with the basic premise that the particularity required in a search warrant is based upon the circumstances of the case, the Court disagrees with the Defendant's parsing of the cases. In both Tillotson and the instant case, the search warrant authorizes the seizure of certain types of computer files (there images of child pornography, here email and other computer data relating to computer hacking or other named items) that are unlikely to be named something that would indicate their contents. See id. Moreover, the Tillotson court's analysis of the ongoing nature of the crime related to its analysis of the staleness issue. See id. at *3. There, the court

reasoned that the defendant would be likely to retain the illegal images, thereby reducing the concern that the items sought would no longer be on the computer. Id. In the present case, staleness is not implicated. The agents seized the Defendant's computer on September 20, 2008, a mere four days after the commission of the alleged crime. Although the rubico message attributed to the Defendant indicated that he had deleted the data that he had retrieved from Governor Palin's account, the search warrant affidavit relates that computer files "can be recovered months or even years after they have been downloaded on to a hard drive, deleted or viewed via the internet." Accordingly, the Court finds that the information sought was likely recoverable from the Defendant's computer despite the short duration of the alleged criminal activity.

Based upon its analysis of the relevant case law, the Court concludes that the agents properly seized the Defendant's computer and searched all the files therein for the items listed in paragraph one of Attachment B to the first search warrant. The agent's seizure of all of the data on the computer in order to search it offsite did not exceed the scope of the search warrant.

(iii) Specific items seized outside of the scope of the first search warrant.

In the Government's response [Doc. 72] to the Defendant's second suppression motion, the Government noted repeatedly that the Defendant had not alleged that any specific item seized fell outside the scope of the search warrant. In his reply [Doc. 74, p.4-6] to this response, the Defendant appears[9] to raise for the first time that, even if the agents had authority to peruse every file on his

[9]The exact nature of the Defendant's argument is unclear because this section of his reply bears the heading "THE SEARCH EXCEEDED THE SCOPE OF AUTHORITY" and the main thrust of this section appears to be his contention that an evidentiary hearing is necessary to determine the search methodology used.

computer, the agents exceeded the scope of the search warrant by seizing files unrelated to the offense under investigation. In this regard, the Defendant asserts that the executing agents' examined "malware" (a "sophisticated malicious code that was somehow installed on the computer before Mr. Kernell possessed it") and obtained the following eight items outside the scope of the first search warrant:

> (1) The citibank.com username and password created in March 2008 by Mr. Kernell's aunt and uncle . . .;
>
> (2) Mr. Kernell's aunt's MasterCard account information used to donate to the Narcolepsy Network in April 2008 . . .;
>
> (3) Personal emails to which Mr. Kernell was not [a] party, including emails sent from Mr. Kernell's uncle to Mr. Kernell's aunt[and] from Mr. Kernell's aunt to Mr. Kernell's cousin . . .;
>
> (4) Mr. Kernell's aunt's PayPal log-on and password information from June 2008 . . .;
>
> (5) Messages from Facebook account dated September 4, 2008 . . .;
>
> (6) Information that Mr. Kernell downloaded software for Zune on September 11, 2008, a program manufactured by Microsoft to listen to music . . .;
>
> (7) The results of '[a]n examination for the term "Blackberry"' . . .; and
>
> (8) Information related to the allegation of obstruction of justice rather than the charges listed in the first Warrant . . . .

[Doc. 74, pp. 4-5] He argues that these examples reveal that the executing agents searched the computer in such a way that exceeded the scope of the search warrant.

The Government filed no reply to these new allegations but responded generally at the December 3 hearing that the items raised by the Defendant were seized pursuant to the search warrant as evidence of hacking activities. It argued that the emails and credit card information

relating to the Defendant's aunt and uncle were relevant to who owned the computer at the time of the offense. It contended that the evidence suggested that more than one person was involved in the commission of unauthorized access of Governor Palin's account, thus it was important to establish who owned the computer and when. AUSA Goldfoot explained that the agents investigated malware, a program that created and disseminated a log of user activity, in order to rule out the possibility that someone other than the Defendant gained control of the Defendant's computer and committed the unauthorized access. While admitting that Zune files related to music, Mr. Goldfoot stated that metadata linked to the individual who accessed Governor Palin's account revealed that Zune was installed on the computer used by that individual. He asserted that the fact that Zune files were installed on the Defendant's computer and the date of their installation were relevant to proving that his computer was the one communicating with the relevant websites and, thus, was used to conduct the hacking activities.

The Court finds that examination of the malware, the information regarding the prior users (items 1-4), and the Zune file (item 6) was proper to establish the identity of the individual conducting the hacking activities. The seizure of Facebook messages dated September 4, 2008, (item 5) was proper because Facebook is specifically itemized in paragraph one of the Attachment. An examination of the June 29, 2009 forensic report, which the Defendant filed as a sealed exhibit, reveals that the September 4 message contained a telephone number which matched the Defendant's cellular telephone. The September 4 Facebook message, in conjunction with other information, allowed the analyst to determine that the Defendant was the user of the subject computer from September 2, 2008, forward. The Court finds this information is also relevant to the identity of the person conducting the hacking activities and, thus, within the scope of the search warrant.

With regard to the agents' examination of the term "Blackberry" (item 7), the Court first notes that the Defendant does not allege that any data was "seized" as a result of this search but merely takes issue with the use of that search term. While "Blackberry" seems unrelated to the items listed in Attachment B at first blush, the Court observes that the supporting affidavit states that a poster (later deemed to be the Defendant) to the 4CHAN message board claimed that he "hacked" into Governor Palin's email account and read everything on it, including "every little blackberry confirmation[.]" Thus, the Court finds that a search for the term "Blackberry" could yield evidence of hacking activities, which the agents were permitted to seize pursuant to Attachment B. Moreover, the Court's examination of the June 29, 2009 forensic report revealed that the analyst's examination of the term "Blackberry" led to metadata in a deleted picture file identical to a picture on Governor Palin's account. Accordingly, the examination of this search term yielded evidence that fell within the scope of Attachment B.

Finally, the Defendant claims that agents seized information related to the allegation of obstruction of justice (item 8) rather than the unauthorized access of Governor Palin's email account, which was the crime under investigation in the first search warrant. The Defendant does not state what information was seized in this regard and, thus, the Government has provided no explanation of its seizure. The Court also finds that such information could be properly seized as evidence of hacking activities because the supporting affidavit notes that the individual posting to the 4CHAN message board claimed to have deleted all of the information he gained from Governor Palin's email account. The Court's review of the June 29, 2009 forensic report confirms that the deleted materials referenced were linked to the hacking activities under investigation.

Accordingly, the Court finds that the seizure of the items listed by the Defendant did not

exceed the scope of the search warrant.

(iv) Good faith of executing agents.

Finally, the Defendant contends that the agents did not rely upon the search warrant in good faith because they knew they were seizing thousands of pages of information without probable cause and they neither sought to limit the first search warrant with a search protocol nor did they seek a another, more particularized search warrant after seizing the computer. Accordingly, he argues that the application of the exclusionary rule is warranted in this case. The Government responds that the agents obtained and executed the search warrants in good faith and, thus, the exclusion of the evidence would not serve to deter improper police conduct.

The Court has found that the executing agents acted within the scope of the search warrant in seizing the Defendant's computer and searching through all the files thereon. This finding obviates the need to examine whether the agents relied upon the search warrant in good faith.

(3) Duration of Searches.

At the time that both of the search warrants were executed, Rule 41(e)(2)(A)(i) provided that a search warrant "must command the officer to . . . execute the warrant within a specified time no longer than 10 days." The Defendant contends that the executing agents and forensic analysts violated Rule 41 of the Federal Rules of Criminal Procedure by searching his laptop for more than ten days following the execution of each of the two search warrants. The Court finds that the ten-day limitation on the execution of a search warrant applies to the initial seizure of the computer hardware. "The subsequent analysis of the computer's contents is not a search in the sense

contemplated by Rule 41 of the warrant." Tillotson, 2008 WL 5140773, at *6 (upholding examination of computer's files beyond Rule 41's 10-day limitation of the authority of a search warrant).

In addition to Tillotson, the Eighth Circuit and several district courts have also held that Rule 41's ten-day rule did not limit the subsequent analysis of seized computer files. United States v. Mutschelknaus, 592 F.3d 826, 830 (8th Cir. 2010) (affirming that a sixty-day extension for examination of a seized computer did not violate Rule 41); Matter of the Search of the Scranton Housing Authority, 436 F. Supp. 2d 714, 727 (M.D. Pa. 2006) (holding that a continuing search of computer files did not violate Rule 41, the purpose of which is to prevent stale warrants, because once the computer in question was imaged within the time specified in the warrant, the evidence was "frozen in time" alleviating the concern that probable cause would have ceased to exist), vacated on other gnds, 487 F. Supp. 2d 530 (M.D. Pa. 2007); United States v. Hernandez, 183 F. Supp. 2d 468, 480 (D.P.R. 2002) (holding that "[n]either Fed. R. Crim. P. 41 nor the Fourth Amendment provides for a specific time limit in which a computer may undergo a government forensic examination after it has been seized pursuant to a search warrant"); United States v. Triumph Capital Group, Inc., 211 F.R.D. 31, 66 (D. Conn. 2002) (holding with regard to the analysis of computer data, Rule 41 does not impose "any time limitation on the government's forensic examination of the evidence seized").

Relying upon United States v. Mitchell, 565 F.3d 1347, 1351 (11th Cir. 2009), the Defendant argues that Rule 41 does not contain an exception for computers. In Mitchell, the Eleventh Circuit held that the search of a computer hard drive pursuant to a search warrant obtained twenty-one days after the warrantless seizure of the hard drive was unreasonable. Mitchell, 565 F.3d at1351. The Court finds this case to be inapposite to the instant analysis. The Eleventh Circuit's decision turns

upon the reasonableness of the defendant being deprived of his "possessory interest" in his hard drive for twenty-one days *with no search warrant in place*, not the reasonableness of the duration of the analysis of electronic data seized pursuant to a search warrant. See id. at 1351-52. In the instant case, the Court finds that the agents seized the evidence pursuant to the first search warrant and within the ten-day time limitation of Rule 41.

Finally, the Court notes that Rule 41 has now been amended to reflect the distinction between the time the computer data is seized and the time that it is analyzed:

> A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

Fed. R. Crim. P. 41(e)(2)(B) (effective Dec. 1, 2009). The commentary to the new rule explains that

> [c]omputers and other electronic storage media commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information during execution of the warrant at the search location. This rule acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant.
>
> . . . .
>
> In addition to addressing the two-step process inherent in searches for electronically stored information, the Rule limits the [now fourteen-] day execution period to the actual execution of the warrant and the on-site activity. While consideration was given to a presumptive national or uniform time period within which any subsequent off-site copying or review of the media or electronically stored information would take place, the practical reality is that there is no basis for a "one size fits all" presumptive period. A substantial amount of time can be involved in the forensic imaging and review of information. This is due to the sheer size of the storage capacity of media, difficulties created by encryption and booby traps, and the workload of the computer labs. The rule does not prevent a judge from

> imposing a deadline for the return of the storage media or access to the electronically stored information at the time the warrant is issued. However, to arbitrarily set a presumptive time period for the return could result in frequent petitions to the court for additional time.

Fed. R. Crim. P. 41(e)(2)(B), Committee Comments to the 2009 Amendments. The Court likewise finds that applying the ten-day time limitation in Rule 41 to the seizure or imaging of the computer files, rather than their subsequent analysis, advances the safeguards intended for the computer's owner/user while recognizing the practical challenges inherent in analyzing electronically stored data.

Accordingly, the Court finds that the forensic analysis of the data on the Defendant's computer without a written search methodology and in excess of the ten-day time limitation in Rule 41 does not violate the Fourth Amendment.

B. Particularity of First Search Warrant

The Defendant also argues that the first search warrant is not sufficiently particular in either the items to be seized or the places to be searched because it does not limit the executing computer analyst to search for only those items for which there is probable cause and in only those locations on the computer where those items might be found.

The Fourth Amendment requires that a search warrant "particularly describ[e] the place to be searched and the persons or things to be seized." U.S. Const. am. IV. The particularity requirement forecloses the opportunity for a general search and "prevents the seizure of one thing under a warrant describing another" by restricting the discretion of the executing officer. Marron v. U.S., 275 U.S. 192, 196 (1927). "However, the degree of specificity required is flexible and will vary depending on the crime involved and the types of items sought." United States v. Henson, 848

F.2d 1374, 1383 (6th Cir. 1988). The description of items to be seized pursuant to a search warrant is sufficient "'if it is as specific as the circumstances and the nature of the activity under investigation permit.'" Id. (quoting United States v. Blum, 753 F.2d 999, 1001 (11th Cir. 1985)).

In the present case, the first search warrant authorizes the search of the Defendant's bedroom and the common areas of his apartment, as particularly described in Attachment A. Attachment B lists the items to be "searched and seized from the premises described in Attachment A." Paragraph one, which is quoted above, permits the seizure of

> Documents and computer files any in [sic.] form including but not limited to e-mail, documentation or papers, and digital data that may [be] related or be associated the screen nicknames rubico and rubico10, the e-mail accounts rubico@yahoo.com and rubico10@yahoo.com, dkrocket@mindspring.com, gov.palin@yahoo.com; Governor Sarah Palin; Facebook; other internet accounts or online services or groups, or hacking activities.

Paragraph two authorizes the seizure of an "Acer brand laptop computer[,]" and paragraph three allows for "[r]eceipts for internet service." Paragraph four lists "[r]ecords, notes, emails, journals, stories, or other forms of documentation of activities related to or referring to the e-mail addresses of or the name Sarah Palin." Paragraph five relates to documentation associating the Defendant's bedroom with him. Paragraphs six, seven, eight, nine, and ten permit the seizure of computer equipment, computer hardware, computer software, instructional computer manuals, and computer passwords/security devices respectively.

1. Particularity in Items to be Seized.

First, the Defendant argues that the search warrant was overly broad because it permitted the seizure of items for which there was no probable cause, namely all of the data in the defendant's computer that did not relate to the items listed in Attachment B, thereby transforming the search warrant into a general warrant. Next, he claims that the list of items to be seized itself is overly broad. Specifically, he challenges the language of paragraph one of Attachment B, that the officers may seize documents and computer files related to "internet accounts or online service groups, or hacking activities[.]" He argues that the other more specific items listed in paragraph one, such as specific screen nicknames or email accounts, are subsumed by this broad concluding language. In his supplements, he argues that the overbreadth of these terms and of Attachment B is not saved by a reference to the crime under investigation. Thus, he contends that the proper remedy for an overly broad search warrant is suppression of all of the evidence gained therefrom. The Government responds that the search warrant properly authorized the seizure of the Defendant's computer as an instrumentality of the crime. It also contends that the first search warrant authorized the seizure of computer files "related to particular online names and records relating to the attack on Governor Palin's account." [Doc. 22, p.8] It maintains that such specification met the Fourth Amendment's particularity requirement because it is "'as specific as the circumstances and the nature of the activity under investigation permit.'" [Doc. 22, p. 8 (quoting United States v. Campbell, 256 F.3d 381, 389 (6th Cir. 1999)] Finally, it argues that Attachment B's list of items to be seized, which was expressly incorporated into and attached to the search warrant, was sufficiently particular even without a specific reference to the crime of unauthorized access of a computer.

"General warrants that fail to describe with particularity the things to be searched for and

seized 'create a danger of unlimited discretion in the executing officer's determination of what is subject to seizure and a danger that items will be seized when the warrant refers to other items.'" Henson, 848 F.2d at 1382 (quoting United States v. Savoca, 761 F.2d 292, 298-99 (6th Cir.), cert. denied, 474 U.S. 852 (1985)). The Court finds that the first search warrant is not a general warrant, as the Defendant alleges, because it does particularly describe the types of items to be seized. First, the search warrant expressly permits the seizure of an Acer laptop computer. As discussed above the Sixth Circuit has affirmed the constitutionality of the seizure of the entire contents of a computer for an offsite search. Guest, 255 F.3d at 334-35. Moreover, as noted by the Government, the Tillotson court also addressed the instant argument, that the seizure of the computer and all the data contained thereon violated the particularity requirement of the Fourth Amendment. Tillotson, 2008 WL 5140773, at *5. Rejecting this contention, the court held that because the pornography, which was the object of the search, "could be located in files with misleading names, authorizing a search of all files on the computer was as specific as the warrant could be under the circumstances." Id.

Second, the search warrant specifies the types of computer data that may be seized from the Defendant's computer. The Court finds that the items listed in paragraph one of Attachment B are as specific as allowed by the circumstances and the crime under investigation. The affidavit supporting the first search warrant states that the affiant was investigating the Defendant's compromise of Governor Sarah Palin's personal email account in violation of 18 U.S.C. §1030(a)(2)(C) and (c)(2)(B). The affidavit relates that on September 16, 2008, an anonymous individual posted a message on an internet message board, claiming that the author had compromised Palin's email account and changed the password to another term, which it then discloses. The affidavit then describes how the affiant identified the anonymous author of the

September 16 message to be the Defendant, including the description of a September 17 message by "rubico" explaining how he had accomplished the "hack[,]" and the connection of the "rubico" post to the accounts "rubico10@yahool.com" and "dkrocket@mindspring.com." The affidavit also states that the Defendant's roommates reported that he had a Facebook account, that he admitted that he made the "rubico" posting, and that the Defendant used the nickname "rubico" when playing on X-Box Live. Thus, the Court finds that the items listed in paragraph one are sufficiently particular given the criminal activity under investigation.

With regard to the alleged expansive reach of the language "internet accounts or online service groups" in paragraph one, the Court first observes that the Defendant has not pointed to any particular data that was seized only because it related to an internet account or an online service group.[10] Additionally, the Court finds that the grouping of this language with "hacking activities" as another item in the larger series prevents the seizure of computer data relating only to other internet accounts or other online service groups unless those items are also connected to hacking activities. The use of general or "generic" terms in a search warrant does not automatically vitiate the warrant's particularity. Henson, 848 F.2d at 1383 (using generic classes of items is sufficient when the officer applying for the warrant has no way to know what specific records will contain the information sought). Additionally, items to be seized may be construed in relation to each other. See Andresen v. Maryland, 427 U.S. 463, 480-81 (1976). In Andresen, the meaning of the term "crime" was limited by its context and position in the search warrant's list of items to be seized. Id. The Court concluded the term "crime" referred to the "crime of false pretenses" as to a specific

[10]In this regard, the Court again notes that its decision not to hold an evidentiary hearing does not prevent the Defendant from comparing the forensic reports listing the computer data seized with the items listed in Attachment B.

property because of its placement at the end of the list of specific items, which were all preceded by a reference to the specific crime and property. Id. at 481-82. Similarly, the terms "other internet accounts or online services or groups" can be construed by their relation to the other term in that portion of the list "hacking activities."

At the December 3 hearing, the Defendant also argued that the term "hacking activities" is overly broad because it essentially permitted the forensic analysts to search for anything they deemed to be generally related to the case. He contends that because "hacking activities" can be read so broadly, it does not limit the agent's discretion. The Court disagrees. The term "hacking activities" clearly limited the executing agents to documents or computer files related to or associated with breaking into or unauthorized access of a computer or an electronic account or information.[11] See generally, United States v. Gray, 78 F. Supp. 2d 524, 529 & n.7 (E.D. Va. 1999) (discussing search of computer for certain documents and "hacker materials," which was how the court characterized the search for "utilities that would enable defendant to access protected computers without authorization). While the term might have permitted the seizure of a large amount of computer data, such does not mean that the term was overly broad. The Court finds that the first search warrant was sufficiently particular with regard to the items to be seized.

Finally, in his supplemental filings [Docs. 76 and 101], the Defendant faults the search warrant for failing to limit the items to be seized with a reference to the crime under investigation. Quoting a recent case from the District Court for the Eastern District of New York, he argues that

[11]As stated above, the affidavit supporting the first search warrant described a September 17 message by rubico (later deemed to be the Defendant) explaining how he had accomplished the "hack" of Governor Palin's account, which in the context of particularity supports the Court's finding that the meaning of the term is clear.

"'whatever new challenges computer searches pose in terms of particularity, it is always necessary–and hardly onerous–to confine *any* search to evidence of particular crimes.'" [Doc. 101, p.1 (quoting United States v. Cioffi, No. 08-CR-415, 2009 WL 3738314, *5 (E.D.N.Y. Nov. 2, 2009)] In Cioffi, the search warrant authorized the seizure of items referenced in an attachment, which included all email in the defendant's personal email account through a certain date, but did not limit the emails subject to seizure to those containing evidence of the charged crimes. Id. at 389. The search warrant did not list the charged crimes and did not incorporate the supporting affidavit, which incorporated the indictment. Moreover, the attachment did not specify any search protocol for the agent to follow in searching and seizing particular data from the defendant's account. Id. The court noted that the Ninth Circuit and some commentators had endorsed the use of a search protocol in the warrant to limit a computer search's intrusion into irrelevant and innocent materials but stated that "the majority of courts to have considered the question have not required the government to specify its search protocol in advance." Id. at *5. Ultimately, the court did not weigh in on this question, but instead held that the warrant constituted a general warrant because it failed to particularize the items to be seized by reference to the charged crimes. Id. (observing that a warrant authorizing the search for evidence of any crime is the very definition of a general warrant).

Defendant Kernell argues that the instant search warrant violates the particularity requirement for the same reasons as the search warrant in Cioffi because it does not set out a search protocol, limit the items to be seized by reference to a crime, or incorporate and attach the supporting affidavit. In this regard, he contends that "[i]f probable cause to seize a computer is held to authorize a search of all that computer's contents– without reference to a specific crime or the type of evidence sought– then any limitations imposed by the magistrate to curb the officer's

discretion, as required by the Fourth Amendment, would have been erased from the warrant's face once the computer was seized." [Doc. 101, pp.4-5]

The Government contends that Cioffi does not apply to the present determination because unlike the Cioffi warrant, the first search warrant in the instant case particularizes the items to be seized by specifying the evidence sought and referring to the crime generally as "hacking activity." It argues that the search warrant incorporates Attachment B. Thus, the search warrant does not permit the executing agents to search for evidence of any crime but, instead, limits their discretion to records or files identified by subject matter. The Government explains that the degree of particularity in the search warrant is not less because the Attachment "uses the plain-English word 'hacking' rather than a Bluebook citation to the precise part of the United States Code that prohibits hacking; with or without a statutory citation, the warrant still commanded the officer to limit himself to evidence of hacking." [Doc. 102, p.2]

The Court agrees with the Government that in the instant case, there is no need to look to the affidavit for particularization of the items to be seized because the incorporated attachment sufficiently specifies the evidence sought. See United States v. Brown, 49 F.3d 1162, 1169 (6th Cir. 1995) (holding that the seizure of items not specifically named in the search warrant did not violate the Fourth Amendment because those items were reasonably related to the offense forming the basis for the search warrant even though that crime was not named in the search warrant itself); see also id. at 1173-74 (Batchelder, J., dissenting).[12] In the present case, the list of items to be seized in

[12]Although Judge Batchelder determined that a search warrant must particularize the crime occasioning the search as well as the places to be searched and the things to be seized, she held that specificity in the items to be seized can make up for a lack of particularity in the crime: "[A] warrant is facially invalid if it neither particularly describes the places to be searched and the things to be seized nor adequately describes the suspected criminal conduct to which the

Attachment B is sufficiently specific in enumerating the items to be seized that it compensates for the absence of a description of the crime on the face of the search warrant. Moreover, the Court finds that the term "hacking activities" is a general reference to the crime under investigation and is perhaps more meaningful to both an executing agent and the Defendant whose property is subject to seizure than a citation to the statute.

2. Particularity in Places to Be Searched.

The Defendant also contends that the first search warrant is overly broad because it does not particularize the places on his computer that can be searched but, instead, permits the executing computer analyst to search through every file in the computer. He argues that each packet of information on his computer is the equivalent of a container, and, thus, the opening of each information packet is a separate search. Accordingly, he reasons that probable cause to open some of the information packets or files on his computer does not provide probable cause to open all the files. The Defendant challenges the warrant for placing no searching limitations on the computer analyst such as a date restriction or specifically stating which terms could be searched and a method for searching them. He asserts that the large volume of information contained on a computer and the inherent intermingling of relevant and irrelevant information therein require that search warrants authorizing the search of a computer's contents must carefully delineate the areas of the computer that the agents can search and the types of information for which they can search.

The Government responds that an executing analyst may properly search in any location on the computer large enough to hold the information on the Defendant's unauthorized access, which

---

search is related." Brown, 49 F.3d at 1174 (Batchelder, J. dissenting).

it contends permits the search of the entirety of the files on the computer. It argues that the Defendant's Fourth Amendment rights are protected by the fact that the agents can only search *for* those items particularized in the search warrant, even though they can search *in* any file on the computer.

The Fourth Amendment requires particularization in only two respects: In "the place to be searched" and "the persons or things to be seized." United States v. Grubbs, 547 U.S. 90, 98 (2006). "'Nothing in the language of the Constitution or in [the Supreme] Court's decisions interpreting that language suggests that, in addition to the [requirements set forth in the text], search warrants also must include a specification of the precise manner in which they are to be executed.'" Id. at 99 (quoting Dalia v. United States, 441 U.S. 238, 255 (1979) (first alteration added)). Although the level of particularization necessary in each case turns upon the circumstances and the activity under investigation therein, Henson, 848 F.2d at 1383, the Court observes that the Sixth Circuit has not required such a limiting methodology in discussing the constitutionality of a search of all the files on a computer. Guest v. Leis 255 F.3d 325, 334-35 (6th Cir. 2001). In Guest, which was discussed above with regard to the execution of the instant search, the Sixth Circuit affirmed both the particularity and the execution of the search of a computer, which the court acknowledged involved searching files not listed in the search warrant. Id. In its analysis, the appellate court at no point discusses whether a limiting methodology was in place or suggests that one was required. Id.

Additionally, more recent cases from the Ninth and Tenth Circuits have not required search warrants authorizing the search of a computer to have a limiting methodology for the manner in which the search would be executed. United States v. Hill, 459 F.3d 966, 977 (9th Cir. 2006); United States v. Brooks, 427 F.3d 1246, 1251 (10th Cir. 2005); see also United States v. Cartier, 543

F.3d 442, 447-48 (8th Cir. 2008) (acknowledging that "there may be times that a search methodology or strategy may be useful or necessary" but declining "to make a blanket finding that the absence of a search methodology or strategy renders a search warrant invalid per se"); see generally, United States v. Khanani, 502 F.3d 1281 (11th Cir. 2007) (holding that lack of a written search methodology did not require suppression but observing that agents employed unwritten precautions); United States v. Upham, 168 F.3d 532, 537 (1st Cir. 1999) (observing that the "warrant process is primarily concerned with identifying *what* may be searched or seized–not how"). In Hill, the Ninth Circuit found that requiring a search methodology or protocol in a search warrant would be "unreasonable" due to the fact that a computer user can easily disguise files. Id. at 977. The court explained that it "look[ed] favorably upon the inclusion of a search protocol; but its absence is not fatal." Id. Finally, the Ninth Circuit noted that regardless of the inclusion or absence of a search methodology, the executing officer is always limited by the fact that he or she may not use any search warrant to conduct a "general, exploratory search." Id. (internal quotation omitted). In Brooks, the Tenth Circuit observed that it "has never required warrants to contain a particularized computer search strategy. We have simply held that officers must describe with particularity the objects of their search." 427 F.3d at 1251. The Court finds the reasoning in these cases to be persuasive.

The Defendant argues that an earlier Tenth Circuit case, United States v. Riccardi, requires that computer searches must be conducted in such a way that the officer "'avoids searching the files of types not identified in the warrant.'" 405 F.3d 852, 862 (10th Cir. 2005) (quoting United States

v. Walser, 275 F.3d 981, 986 (10th Cir. 2001)).[13] The inevitable intermingling of relevant and irrelevant files on a computer caused the court to require that "warrants for computer searches must affirmatively limit the search to evidence of specific federal crimes or specific types of material." Id. (observing that the warrants failure to limit the computer search to the seizure of particular files or to any particular crime "permitted the officers to search for anything–from child pornography to tax returns to private correspondence[,]" i.e., to conduct a general exploratory search).

The Court finds that this language does not require that the search warrant particularize a search methodology, as Brooks subsequently explained. See Brooks, 427 F.3d at 1251. "The question of whether the nature of computer forensic searches lends itself to predetermined search protocols is a difficult one. Given the numerous ways information is stored on a computer, openly and surreptitiously, a search can be as much an art as a science." Id. at 1251-52. The Tenth Circuit noted that in cases in which the original search expanded upon discovery of evidence of other crimes during the computer search, it had required additional authorization for an expanded search. Id. at 1252 (citing United States v. Carey, 172 F.3d 1268 (10th Cir. 1999)). Nevertheless, the court

[13]The Defendant also cites to a few district court cases in which the court either suggested, approved, or required the inclusion of limitations on the method of a computer search in the warrant. See In re Search of 3817 W. West End, First Floor, 321 F. Supp. 2d 953 (N.D. Ill. 2004) (refusal to permit search of seized computer without government's provision of a search protocol and finding that a search protocol was necessary to satisfy the particularity requirement under the circumstances of that case); United States v. Barbuto, No. 2:00CR197K, 2001 WL 670930, *5 (D. Utah Apr. 12, 2001) (interpreting 10th Circuit case law to require that agents present a search methodology before searching a computer); United States v. Gawrysiak, 972 F. Supp. 853, 866 (D.N.J. 1997) (suggesting, in dicta, that the executing agent could have copied only those files falling within the relevant dates at the time he imaged the computer in the defendant's home). With regard to these cases, the Court observes that Barbuto relied upon the Tenth Circuit in United States v. Carey, 172 F.3d 1268 (10th Cir. 1999), regarding which the Tenth Circuit subsequently explained in Brooks, 427 F.3d at1251, did not require a search methodology. Moreover, Gawrysiak specifically approves the agent's seizure of all files on the computer for a subsequent offsite search. 972 F. Supp. at 866.

emphasized that these prior cases "do not, however, stand for the proposition that a warrant is per se overbroad if it does not describe a specific search methodology." Id. Finally, the Tenth Circuit held that unlike in Riccardi, the search warrant avoided overbreadth by limiting the search of the defendant's computer with a "subject matter" restriction of "particular items specifically related to child pornography." Id. at 1253. Thus, the Court finds that it is the particularity in the items to be seized that protects the Defendant against the executing agent's unbridled discretion.

The Defendant also argues that the second search warrant for his laptop computer reveals that the Government could have sought a more particular search warrant initially, either by specifying a search protocol in the first search warrant or by immediately seeking another search warrant with a limiting methodology once the computer was in Government custody. The Defendant argues that in seeking a second search warrant in February 2009, the Government admitted[14] that it lacked authority to search the computer under the first search warrant and that a targeted search was possible. He asserts that the Government cannot now take the inconsistent position that the inclusion of a particular search protocol in the first search warrant was unworkable.

The Government responds that the suppression issues raised by the Defendant can be resolved by looking to the first search warrant alone. It contends that the second search warrant, which sought additional judicial review based on new charges against the Defendant, only gave the Defendant additional protection under the Fourth Amendment. It asserts that it sought the second

[14]The Defendant argues that the Government is now judicially estopped from advancing the position that it could search the entire computer before the issuance of the second search warrant in February 2009. Because the Court finds that the Government's seeking of the second search warrant does not represent a position inconsistent with the Government's seeking of the first search warrant, the Court need not reach the question of whether judicial estoppel is proper in this case.

search warrant because of evidence it had obtained in its ongoing investigation of the Defendant and because the Superseding Indictment brought new charges against him. It maintains that obtaining a second search warrant under these circumstances was a "sensible precaution," because some courts have warned against expanding the search's scope without getting another warrant. [Doc. 72, p.11] Finally, the Government points out that the second search warrant does not set out a search protocol.

The Court finds that the Defendant is essentially arguing that because the first search warrant was not as particular as the second search warrant, the first search warrant fails to provide a level of particularity that is as specific as the circumstances required. [See Doc. 69, p.13 (stating that "unnecessary and unjustified extensive searching directly contravenes the purpose of the Fourth Amendment's particularity requirement.")] The flaw in this reasoning is two-fold. First, the second search warrant seeks evidence of five crimes not involved in the first search warrant. Accordingly, the particularization of the items to be seized is different. Thus, if the level of particularity is greater in the second search warrant, it is because the *circumstances* are different. Second, the second search warrant also does not prescribe a search methodology or protocol. The Defendant correctly points out that the affidavit in support of the second search warrant states that "[i]n some cases, it is possible for agents to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence." Nevertheless, the affidavit also states that this case "may involve a range of data analysis techniques[;]" that in some cases, targeted searches "may not yield the evidence described in the warrant" because defendants can hide, mislabel, encrypt, or attempt to delete files; and that the "affiant intends to use whatever data analysis techniques appear necessary to locate and retrieve the evidence" described in the attachment. Thus, although the affidavit supporting the

second search observes that targeted searches are sometimes possible, it in no way limits the search requested therein to a targeted search or imposes any type of search protocol. The language in the second search warrant and its supporting affidavit does not cause the Court to find that the first search warrant was not sufficiently particular with regard to the places to be searched.

In the present case, the affidavit supporting the first search warrant states that a review of the data on the computer can take weeks or even months, depending on the volume of data contained on the computer. It also notes that searching authorities must examine all of the data on the computer to determine whether it contains an item listed in the warrant because a computer's user can store information on the computer using "deceptive file names" or in "random order." Based upon this information and the specificity of the items to be seized, the Court finds that a search of all the files on the Defendant's computer for the items listed in Attachment B was reasonable.[15]

[15]Because the Court does not find the search warrant to be overly broad with regard to its particularization of the places to be searched or the items to be seized, it need not consider the Defendant's claim in his first supplemental brief [Doc. 76], citing United States v. Wecht, 619 F. Supp. 2d 213 (W.D. Pa. 2009), that suppression of all of the evidence is the proper remedy in this case.

IV. CONCLUSION

After carefully considering the motions, memoranda, oral arguments, supplements, and search warrants and supporting documents and after reviewing the relevant legal authorities, the Court finds that probable cause supported the issuance of the search warrant and that the executing agents did not exceed the scope of the search warrants. For the reasons set forth herein, it is **RECOMMENDED** that the Defendant's Motion to Suppress [**Doc. 20**] and Second Motion to Suppress [**Doc. 69**] be **DENIED**.[16]

Respectfully submitted,

s/ C. Clifford Shirley, Jr.
United States Magistrate Judge

[16]Any objections to this report and recommendation must be served and filed within fourteen (14) days after service of a copy of this recommended disposition on the objecting party. Fed. R. Crim. P. 59(b)(2) (as amended). Failure to file objections within the time specified waives the right to review by the District Court. Fed. R. Crim. P. 59(b)(2); see United States v. Branch, 537 F.3d 582, 587 (6th. Cir. 2008); see also Thomas v. Arn, 474 U.S. 140, 155 (1985) (providing that failure to file objections in compliance with the required time period waives the right to appeal the District Court's order). The District Court need not provide de novo review where objections to this report and recommendation are frivolous, conclusive, or general. Mira v. Marshall, 806 F.2d 636, 637 (6th Cir. 1986). Only specific objections are reserved for appellate review. Smith v. Detroit Federation of Teachers, 829 F.2d 1370, 1373 (6th Cir. 1987).